UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/853,913	05/11/2001	Sanguthevar Rajasekaran	20967000410	7607

20350 7590 12/21/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 12/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/853,913	RAJASEKARAN, SANGUTHEVAR	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *10-20,25-27,30-32 and 35-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *10-20,25-27,30-32 and 35-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 10-20, 25-27, 30-32, 35-37 are pending.

2. Amendment filed 09/12/2005 with a request for continued examination has been received and considered.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 10-19, 30-31, 35-36 rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al ("Securing Threshold Cryptosystems against Chosen Ciphertext Attack") and further in view of Schneier ("Applied Cryptography").

As per claims 10, 30, 35, Shoup et al discloses, generating keys, encrypting a secret and distributing the secret to the owners at a custodian computer and receiving k secret owner values from a unique combination of k secret owners then determining a value c that is associated with the unique

combination and determining the secret S using the value c and the k secret owner values (see page 5).

Shoup et al fails to disclose the key generation and encryption technique being multiple-key public-key cryptography (in this case RSA), deleting this information after distribution and generating and storing a database of all keys.

However, Schneier teaches the use of multiple-key public-key cryptography (RSA), deletion of secrets (see page 527 where the K's are the $d_1 \ldots d_n$ times $e_1 \ldots e_n$ and pages 184-185 for the deletion and pages 181-182 for the database of all keys).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's multiple-key, deletion, and database methods in the secret sharing of Shoup et al.

Motivation to do so would have been that RSA is the standard in much of the world (see page 474), old keys and old secrets must be deleted because they are valuable even if never used again (see page 184), and to decrypt information if the person with the key is no longer available (see page 181).

As per claims 11-13, the modified Shoup et al and Schneier system discloses receiving the n secret owner pieces (see Shoup et al page 5) and computing $S' = S^{ef} \bmod N$ for the first time and $S' = S'^{q} \bmod N$ for each time after that (see Schneier page 527

where $d_1 \ldots d_n$ times $e_1 \ldots e_n$ are the $K_1 \ldots K_n$ and since in the applicants case only one of the K's are sent per time it is known that Schneier's method can be done incremental rather than all at once as in the example).

As per claim 14, in order to completely decrypt and restore the secret the correct value from the database must be accessed and used to compute the final exponential and modular operations).

As per claims 15-19, 31, 36, the modified Shoup et al and Schneier system discloses computing $S^{ee'}$ (see Schneier page 527). Claims are 15-19, 31, 36 are rejected as in claims 10-15, 30, 35 above with the above mentioned addition.

5. Claims 20, 32, 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shoup et al further in view of Schneier.

As per claim 20, 32, 37, Shoup et al discloses encrypting a secret, and performing a forward k out of n secret sharing algorithm by a custodian computer, store, distributing and receiving k secret owner values from a unique combination of k secret owners then determining a value c that is associated with the unique combination and determining the secret S using the value c and the k secret owner values (see page 5).

Shoup et al fails to disclose deleting the secret.

However, Schneier teaches deleting a secret (see pages 184-185).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Schneier's deletion method in the secret sharing of Shoup et al.

Motivation to do so would have been that old keys and old secrets must be deleted because they are valuable even if never used again (see Schneier page 184).

6. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Shoup et al and Schneier system as applied to claim 20 above, and further in view of Shamir ("How to Share a Secret").

As per claim 25, the modified Shoup et al and Schneier system fails to disclose dividing the secret into k pieces and performing n polynomial evaluations at n points of a degree-k polynomial using the k pieces of the encrypted secret as polynomial coefficients; wherein each of the k secret owner pieces includes a result of one of the n polynomial evaluations and a corresponding one of the n points.

However, Shamir discloses such a break up (see page 613).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Shamir's method of

polynomial break ups in the modified secret sharing method of Shoup et al and Schneier.

Motivation to do so would have been to create a k out of n threshold scheme (see Shamir page 612).

As per claims 26-27, the modified Shoup et al, Schneier and Shamir system discloses distributing the secret pieces and receiving k out of n of the pieces (see Shoup et al page 5), and performing reverse k out of n secret sharing by solving a system of generated linear equations (see Shamir page 613); assembling and decrypting the pieces to recreate the secret (see Shoup et al page 5).

Response to Arguments

1. Applicant's arguments with respect to the claimed database limitation have been considered but are moot in view of the new ground(s) of rejection.

Applicant's arguments filed 09/12/2005 have been fully considered but they are not persuasive. Applicant argues: Shoup fails to disclose determining a value c that is associated with the unique combination and determining the secret S using the value c and the k secret owner values; and that claims 11-14 recite for example computing S'^{c}.

Regarding Applicant's argument with respect to the value c, Shoup teaches receiving shares and combining these shares, this combination is the value c and is used to determine the secret as seen on page 5 3rd paragraph from the bottom of the page.

Regarding Applicant's argument with respect to computing S'^{c} this is not a claimed limitation and is therefore moot.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER